1. STRATEGIC VISION OF THE OFFICE OF CYBER SECURITY

The strategic vision of the Office of Cyber Security is to become a national center of excellence for the safeguarding of classified and unclassified information on electronic systems and critical cyber infrastructures. This enormous undertaking encompasses policies, procedures, and implementation efforts throughout a large, diverse, and geographically dispersed organization. Key to the Department of Energy's (DOE) success is a uniform implementation of innovative policies and agile solutions across the entire enterprise, coupled with an effective cyber security education program available to all DOE staff and contractors.

1.1 GOALS OF THE OFFICE OF CYBER SECURITY

The Office of Cyber Security has determined that to become a national center of excellence it must be committed to strengthening the DOE cyber security community, strengthening DOE cyber security policy implementation to meet or exceed national standards, and strengthening DOE's internal cyber security infrastructure. DOE will also continue to develop innovative approaches for confronting newly identified threats to the community's information systems. These challenging tasks will require dedication and perseverance, but DOE's Office of Cyber Security is committed to its vision of excellence.

1.2 ACTION STEPS

This Action Plan describes ongoing and future activities under the DOE Cyber Security Program. Historically, the program's activities or action steps have been organized into four functional areas. These four functional areas serve as the Office of Cyber Security's core competencies and have proven to be a highly effective means by which budget planning and program execution activities occur. When cross-matrixed with its Strategic Goals, the relationship provides a series of traceable links between the Office's capabilities and budget, the initiatives resulting from the matching of those resources, and the strategic goals they support. This Action Plan lays out an integrated set of activities over a 2-year period that provides the foundation necessary for attaining the vision of the Office of Cyber Security through achieving the established goals. As illustrated in Figure 1.1, the action steps are organized into the following four functional areas:

- *Planning and Performance Management.* DOE will continue to provide a sound and comprehensive framework for effective implementation of the Cyber Security Program.

- *Education, Training, and Awareness.* DOE will continue to develop a coordinated training program intended to improve job performance by providing managers and staff with not only a practical understanding of cyber security threats and vulnerabilities but also the skills and capabilities to address them.

- *Engineering and Assessments.* DOE will continue to provide departmental cyber security engineering and assessment resources to support day-to-day computer operations throughout DOE and throughout the life cycle of computer systems and the information they process.

- *Technical Development.* The Office of Cyber Security's research and technical development capability is designed to research new, innovative cyber security protection capabilities with the goal of improving the Department's information and cyber security systems. DOE will identify, evaluate, and if needed, develop cyber security tools to protect against current and future cyber-related threats and vulnerabilities. DOE will perform need-based analysis to identify new threats and desired protection capabilities. Commercial off-the-shelf (COTS) security software will also be evaluated in a DOE environment, and research and development (R&D) will be conducted to address long-term cyber security needs. DOE-developed tools will be used to provide capabilities not being met by commercial or other government cyber security products.

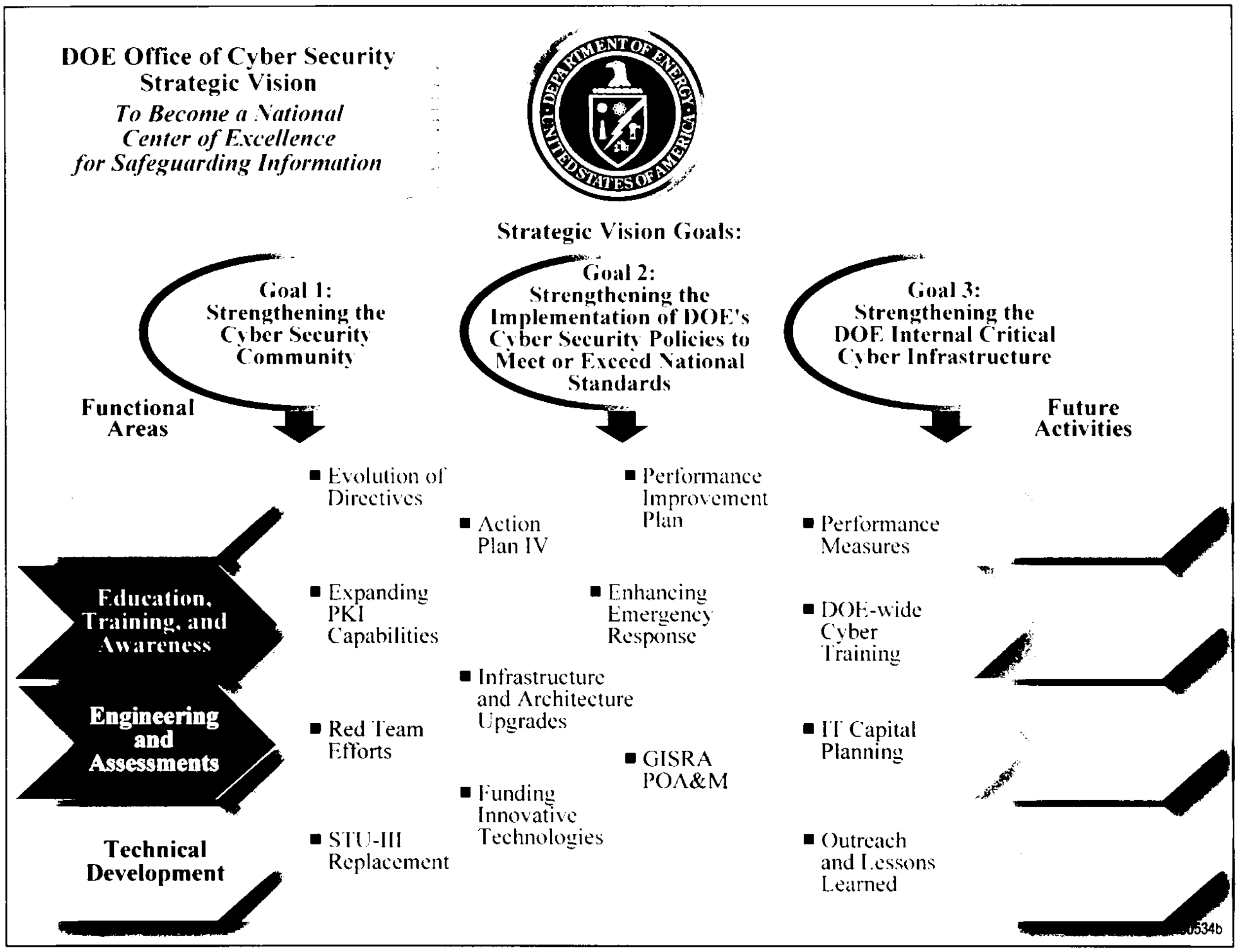
DOE Office of Cyber Security Strategic Vision
To Become a National Center of Excellence for Safeguarding Information
Strategic Vision Goals:
Goal 1: Strengthening the Cyber Security Community
Goal 2: Strengthening the Implementation of DOE's Cyber Security Policies to Meet or Exceed National Standards
Goal 3: Strengthening the DOE Internal Critical Cyber Infrastructure
Functional Areas
Future Activities
Education, Training, and Awareness
Engineering and Assessments
Technical Development
■ Evolution of Directives
■ Action Plan IV
■ Performance Improvement Plan
■ Performance Measures
■ Expanding PKI Capabilities
■ Enhancing Emergency Response
■ DOE-wide Cyber Training
■ Infrastructure and Architecture Upgrades
■ Red Team Efforts
■ GISRA POA&M
■ IT Capital Planning
■ Funding Innovative Technologies
■ STU-III Replacement
■ Outreach and Lessons Learned
0534b

Figure 1-1. DOE Office of Cyber Security Strategic Vision

The Office of Cyber Security has established the following initiatives to support the three main goals of the CIO:

Goal 1—Strengthening the DOE cyber Security Community

1.1 Continue with the development of the action plan to promote and support DOE's vision.

1.2 Define roles and responsibilities for Headquarters and line organizations.

1.3 Ensure that E-Government Initiatives are secure and responsive to the public.

1.4 Update the agencywide Cyber Security Threat Statement to include new threat information based on recent world events.

Goal 2—Strengthening the implementation of DOE cyber security policies to meet or exceed national standards

2.1 Deploy a DOE-wide performance metrics program to provide an assessment of real-time implementation of cyber security programs and to improve security policies where enhancement is warranted.

2.2 Develop and maintain and update the Government Information Security Reform Act (GISRA) Plan of Action and Milestones (POA&M) for the Office of Management and Budget (OMB). This report describes the Chief Information Officer's (CIO) plan to strengthen DOE's cyber security program by ensuring weaknesses identified by internal and external audits are tracked from identification to resolution.

2.3 Develop a cyber security information technology (IT) capital planning process to ensure cyber security dollars are appropriately managed, reviewed, and funded to facilitate the full integration of security into the IT life cycle.

2.4 Continue with the evolution of DOE cyber security guidance directives.

2.5 Expand the Outreach/Lessons Learned program with the continued publication of the CIO's Office of Cyber Security Cyber Security Daily New Brief and publication of the "best practices" papers.

2.6 Develop and expand a comprehensive DOE-wide cyber training program, including forensics awareness training, a recognition program, and a catalog of courses.

Goal 3—Strengthening the DOE internal critical cyber infrastructure

3.1 Continue to support the Computer Incident Advisory Capability (CIAC) in its mission to assist any DOE element that experiences a computer security incident by providing analysis, response, and restoration of operation.

3.2 Expand public key infrastructure (PKI) capabilities throughout DOE to support trusted relationships among all users.

3.3 Fund a Secure Telephone Unit-Third Generation (STU-III) replacement at 25 percent of assets annually over the next 4 years.

3.4 Continue to fund DOE-wide infrastructure and architecture upgrades.

3.5 Fund innovative technologies to ensure practical and enhanced cyber security protection capabilities.

3.6 Transition a Counterintelligence project (Intrusion Monitoring Analysis and Correction [IMAC]) that improves the ability to forecasts upcoming attacks to the Office of Cyber Security.

3.7 Continue with Step 2 of the Project Matrix Initiative.

Table 1-1 provides a brief crosswalk of the activities that support the four functional areas and the strategic goals of the Office of Cyber Security.

Table 1.1. Activity Crosswalk

Functional Area	Goal #1	Goal #2	Goal #3
Planning and Performance Management	1.2 1.3	2.1 2.3 2.4 2.5	3.5
Education, Training and Awareness	1.2 1.3	2.6 2.4	3.1 3.2
Engineering and Assessments	1.1 1.2 1.3 1.4	2.4 2.6 2.4	3.1 3.4 3.6 3.7
Technology Development	1.3	2.2 2.6	3.1 3.2 3.3 3.4 3.5 3.6